What is claimed is:

1. A wireless device comprising:

at least one biometric sensor to obtain biometric information about a user presently holding said wireless device when said wireless device is being held;

a biometric authentication unit to determine, based on said biometric information, whether said user presently holding said wireless device is authorized to use said wireless device;

a wireless transceiver to support wireless communication with a remote entity; and

a controller to control operation of said wireless device, wherein said controller is programmed to change operational characteristics of said wireless device based on whether said wireless device is presently being held.

2. The wireless device of claim 1, wherein:

said controller is programmed to request access to a network, using said wireless transceiver, when said wireless device is being held and said biometric authentication unit indicates that said user presently holding said wireless device is authorized to use said wireless device.

3. The wireless device of claim 2, wherein:

said controller includes information identifying said user presently holding said wireless device as part of said request.

4. The wireless device of claim 2, wherein:

said controller includes biometric information obtained by said at least one biometric sensor as part of said request.

5. The wireless device of claim 2, wherein:

said controller is programmed to prompt said user presently holding said wireless device when network access has been denied.

6. The wireless device of claim 1, wherein:

said controller is programmed to deactivate user functions of said wireless device when said wireless device is being held and said biometric authentication unit indicates that said user presently holding said wireless device is not authorized to use said wireless device.

7. The wireless device of claim 1, wherein:

said controller is programmed to place said wireless device in a power save mode when said wireless device is not being held.

8. The wireless device of claim 1, wherein:

said controller is programmed to place said wireless device in a normal power mode when said wireless device is being held.

9. The wireless device of claim 1, further comprising:

a storage medium to store user profiles for multiple authorized users of said wireless device, wherein said controller loads a profile corresponding to said user presently holding said wireless device from said storage medium into a processor memory after said biometric authentication unit indicates that said user presently holding said wireless device is authorized to use said wireless device.

10. The wireless device of claim 1, wherein:

said controller is programmed to request access to a network for use in performing background functions, using said wireless transceiver, when said wireless device is not being held and when power is sufficient to perform said background functions.

11. The wireless device of claim 10, wherein:

said controller is programmed to enable performance of background functions after network access has been obtained.

12. The wireless device of claim 1, further comprising:

an accelerometer to monitor movement of said wireless device, wherein said controller is programmed to use readings of said accelerometer to determine whether said wireless device is currently being held.

13. The wireless device of claim 1, wherein:

said controller is programmed to use readings of said at least one biometric sensor to determine whether said wireless device is currently being held.

14. The wireless device of claim 1, wherein:

said at least one biometric sensor includes at least one of the following: a fingerprint sensor, a skin temperature sensor, a skin texture sensor, a hand geometry sensor, a voice print sensor, and a heartbeat sensor.

15. A method comprising:

sensing that a wireless device has been picked up by a user;

determining, after sensing that said wireless device has been picked up, whether said user is authorized to use said wireless device based on collected biometric information; and

when said user is determined to be authorized to use said wireless device, requesting access to a network via a wireless link.

16. The method of claim 15, further comprising:

enabling a normal power mode of said wireless device after sensing and before determining.

17. The method of claim 15, further comprising:

when said user is determined to not be authorized to use said wireless device, de-activating user functions of said wireless device.

18. The method of claim 15, further comprising:

when said user is determined to be authorized to use said wireless device, loading a profile associated with said user into a processor memory.

19. The method of claim 15, further comprising:

when access to said network has been granted, loading a profile associated with said user into a processor memory.

20. The method of claim 15, further comprising:

when access to said network has been granted, allowing said user to perform network based functions.

21. The method of claim 15, further comprising:

when access to said network has been denied, prompting said user to indicate same.

22. The method of claim 15, further comprising:

when access to said network has been denied, allowing said user to perform local functions, but not network based functions.

23. A method comprising:

sensing that a wireless device is no longer being held by a user; and

dropping user authentication and network authorization for the device, if any, based on said device no longer being held.

24. The method of claim 23, wherein:

dropping user authentication and network authorization includes waiting a predetermined time period after sensing that said wireless device is no longer being held before dropping said user authentication and said network authorization to allow time for a user to pick said wireless device back up.

25. The method of claim 23, further comprising:

activating a power save mode of said wireless device after sensing that said wireless device is no longer being held.

26. The method of claim 23, further comprising:

requesting access to a network for use in performing background functions after sensing that said wireless device is no longer being held.

27. The method of claim 26, further comprising:

waiting for a power level of said wireless device to be sufficient for performing background functions before requesting access to said network.

28. The method of claim 26, further comprising:

allowing background functions to be performed after access to the network has been granted.

29. A method comprising:

detecting unauthorized use of a wireless device;

determining, in response to detecting, whether said wireless device has been reported lost or stolen; and

when said wireless device is determined to have been reported lost or stolen:

determining a location of said wireless device; and

when said location of said wireless device is not an expected location, backing up data from said wireless device to a remote location.

30. The method of claim 29, further comprising:

sending a data destruct signal to said wireless device to destroy data stored thereon after backing up said data.

31. The method of claim 29, further comprising:

when said location of said wireless device is an expected location, disabling user accessible functions of said wireless device.

32. The method of claim 31, further comprising:

sending reactivation instructions to said wireless device after disabling said user accessible functions of said wireless device.

33. The method of claim 29, further comprising:

when said wireless device is determined to have not been reported lost or stolen, disabling user accessible functions of said wireless device.

34. The method of claim 29, wherein:

determining whether said wireless device has been reported lost or stolen includes consulting a list of devices reported lost or stolen that is maintained at a network location.

35. The method of claim 34, wherein:

consulting a list of devices reported lost or stolen includes consulting an equipment identity register (EIR).

36. The method of claim 29, wherein:

determining a location of said wireless device includes consulting a list of device locations that is maintained at a network location.

37. The method of claim 36, wherein:

consulting a list of device locations includes consulting a mobile location server.

38. A system comprising:

a network access authorization unit to manage network access authorization for wireless devices in a network;

an equipment identity register (EIR) to maintain a list of wireless devices that have been reported lost or stolen, said EIR being accessible by said network access authorization unit;

a backup server to manage data backups for wireless devices in said network; and

a mobile location server (MLS) to track locations of wireless devices in said network;

wherein said network access authorization unit is configured to determine whether a first wireless device has been reported lost or stolen when unauthorized use of said first wireless device has been detected and to determine a location of said first wireless device when it is determined that said first wireless device has been reported lost or stolen.

39. The system of claim 38, wherein:

said network access authorization unit is programmed to instruct the backup server to backup data from said first wireless device when said location of said first wireless device is not an expected location of said first wireless device.

40. The system of claim 39, wherein:

said network access authorization unit is programmed to send a data destruct signal to said first wireless device after said backup server has completed the backup of data from said first wireless device to destroy data stored within said first wireless device.

41. The system of claim 39, wherein:

said expected location includes a home location of a user associated with said first wireless device.

42. The system of claim 39, wherein:

said expected location includes a work location of a user associated with said first wireless device.

43. The system of claim 38, wherein:

said network access authorization unit is programmed to send a disable signal to said first wireless device to disable user accessible functions therein when said location of said first wireless device is an expected location.

44. The system of claim 43, wherein:

said network access authorization unit is programmed to send reactivation instructions to said first wireless device after sending said disable signal.

45. The system of claim 43, wherein:

said network access authorization unit is programmed to: (a) receive a signal from said first wireless device indicating that said first wireless device is no longer being held by a user, (b) start a timer in response to said signal, and (c) deny network access to said first wireless device after said timer has indicated that a predetermined amount of time has passed without said first wireless device being picked up by a user.

46. An article comprising a storage medium having instructions stored thereon that, when executed by a computing platform, operate to:

sense that a wireless device has been picked up by a user;

determine, after sensing that said wireless device has been picked up, whether said user is authorized to use said wireless device based on collected biometric information; and when said user is determined to be authorized to use said wireless device, request access to a network via a wireless link.

47. The article of claim 46, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

enable a normal power mode of said wireless device after sensing and before determining.

48. The article of claim 46, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

when said user is determined to not be authorized to use said wireless device, de-activate user functions of said wireless device.

49. The article of claim 46, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

when said user is determined to be authorized to use said wireless device, load a profile associated with said user into a processor memory.

50. The article of claim 46, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

when access to said network has been granted, load a profile associated with said user into a processor memory.

51. An article comprising a storage medium having instructions stored thereon that, when executed by a computing platform, operate to:

sense that a wireless device is no longer being held by a user; and

drop user authentication and network access for the wireless device, if any, based on said wireless device no longer being held.

52. The article of claim 51, wherein:

to drop user authentication and network access includes to wait a predetermined time period after sensing that said wireless device is no longer being held before dropping user authentication and network access to allow time for the user to pick said wireless device back up.

53. The article of claim 51, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

activate a power save mode of said wireless device after sensing that said wireless device is no longer being held.

54. The article of claim 51, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

request access to a network for use in performing background functions after sensing that said wireless device is no longer being held.

55. The article of claim 54, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

wait for a power level of the device to be sufficient for performing background functions before requesting access to the network.

56. The article of claim 54, wherein said storage medium further includes instructions that, when executed by the computing platform, operate to:

allow background functions to be performed after access to the network has been granted.

57. A wireless device comprising:

at least one biometric sensor to obtain biometric information about a user presently holding said wireless device when said wireless device is being held;

a biometric authentication unit to determine, based on said biometric information, whether said user presently holding said wireless device is authorized to use said wireless device;

a wireless transceiver to support wireless communication with a remote entity;

a controller to control operation of said wireless device, wherein said controller is programmed to change operational characteristics of said wireless device based on whether said wireless device is presently being held; and

at least one dipole antenna coupled to said wireless transceiver to provide a transition to free space.

58. The wireless device of claim 57, wherein:

said controller is programmed to request access to a network, using said wireless transceiver, when said wireless device is being held and said biometric authentication unit indicates that said user presently holding said wireless device is authorized to use said wireless device.

59. The wireless device of claim 57, wherein:

said controller is programmed to place said wireless device in a power save mode when said wireless device is not being held.

60. The wireless device of claim 57, wherein:

said controller is programmed to place said wireless device in a normal power mode when said wireless device is being held.